



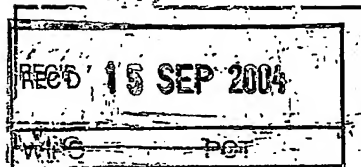
PCT / IB 04 / 03573

12 NOV 2004



INVESTOR IN PEOPLE

The Patent Office  
Concept House  
Cardiff Road  
Newport  
South Wales  
NP10 8QQ



I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

**PRIORITY  
DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

Signed

*Andrew Gersey*

Dated 26 October 2004

**BEST AVAILABLE COPY**



The  
Patent  
Office

22OCT03 EB46375-1 000068  
P01/7700 0.00-0324597.4

The Patent Office

Cardiff Road  
Newport  
South Wales  
NP9 1RH

# Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

1. Your reference	304655GB/PRS/GJS/sjr		
2. Patent application number (The Patent Office will fill in this part)	21 OCT 2003	0324597.4	
3. Full name, address and postcode of the or of each applicant (underline all surnames)	NOKIA CORPORATION KEILALAHDENTIE 4 02150 ESPOO FINLAND		
Patents ADP number (if you know it)			
If the applicant is a corporate body, give the country/state of its incorporation	FINLAND	765227001	
4. Title of the invention	A Communication System		
5. Name of your agent (if you have one)	PAGE WHITE & FARRER 54 Doughty Street London WC1N 2LS		
"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)			
Patents ADP number (if you know it)	1255003		
6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number	Country	Priority application number (if you know it)	Date of filing (day / month / year)
7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application	Number of earlier application	Date of filing (day / month / year)	
8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if: a) any applicant named in part 3 is not an inventor, or b) there is an inventor who is not named as an applicant, or c) any named applicant is a corporate body. See note (d))	Yes		

## Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description

32 —

Claim(s)

3 —

Abstract

Drawing(s)

10. If you are also filing any of the following, state how many against each item.

Priority documents

Translations of priority documents

Statement of inventorship and right to grant of a patent (*Patents Form 7/77*)

Request for preliminary examination and search (*Patents Form 9/77*)

Request for substantive examination (*Patents Form 10/77*)

Any other documents  
(*please specify*)

11.

I/We request the grant of a patent on the basis of this application.

Signature

Date 21.10.03

PAGE WHITE & FARRER

12. Name and daytime telephone number of person to contact in the United Kingdom

P R Slingsby  
020 7831-7929

### Warning

*After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.*

### Notes

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*
- Write your answers in capital letters using black ink or you may type them.*
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*
- If you have answered 'Yes' Patents Form 7/77 will need to be filed.*
- Once you have filled in the form you must remember to sign and date it.*
- For details of the fee and ways to pay please contact the Patent Office.*

## DESCRIPTION OF THE INVENTION

### 1. Field of technology and background

SIP is the Session Initiation Protocol as defined by the IETF in RFC 3261. It allows the establishment, handling and release of end-to-end multimedia sessions. There are several additions to the SIP protocol, which e.g. allow event notification based on SIP, which is the basis for a SIP based Presence Service and other services.

IMS is the 3GPP IP Multimedia Subsystem, that makes use of SIP as its call control protocol. See TS 23.228, 24.229 and 24.228. We hereby incorporate and the reader is referred to 3GPP specifications 23.228, 24.229 and 24.228.

#### Problem

Scenario: A user has successfully registered to the S-CSCF and was authenticated. During the users active registration, the S-CSCF goes out of service.

#### Problems:

- How can another S-CSCF be selected by the I-CSCF?
- How to handle the active dialogs that the user has established with other users and ASs?
- How to inform other network entities (AS / P-CSCF) about the new registration of the user to a new S-CSCF

### 2. Invention

Two scenarios are important:

(1) I-CSCF detects that the S-CSCF is out-of-service during users re-registration

- In this case the I-CSCF sends back a 504 (Server Time-Out) to the UE (1<sup>st</sup> part of invention).
- The UE then drops the signalling (or, if only a general PDP ctx was established, the general) PDP context. (2<sup>nd</sup> part of invention)
- The UE then acts as if it just had re-booted, i.e. it establishes a new general / signalling PDP ctx and performs initial registration.

With this behaviour, all states in the network are also cleared, so all the above mentioned problems are solved.

(2) P-CSCF detects that the S-CSCF is out-of-service during a (non-REGISTER) request sent from the user

- In this case the P-CSCF send back a 504 (Server Time-Out) to the UE
- The UE now cannot be sure, if its own S-CSCF is out of service or another network element on the route towards the destination of the initial request.
- Therefore the UE performs a re-registration whenever it receives a 504 (Server Time-Out) response to any request other than a REGISTER request (3<sup>rd</sup> part of invention)
- The I-CSCF will now behave exactly as described in scenario (1)

It is important to note, that dropping the signalling PDP context is a heavy procedure, as it leads to a complete break in service provision to the user and all the remote users, the user is connected to. On the other hand, service could anyhow not be continued to be provided, as the S-CSCF is out of order. As it is assumed that S-CSCF will go out of order in very very rare cases, this behaviour seems to be suitable for the situation.

A very high sophisticated UE implementation might want to only drop the signalling PDP ctx, but not the media PDP ctxs. This would allow the UE to "go on talking" with the remote side, whilst the

new S-CSCF is selected. Nevertheless this UE would then need to switch over the kept media PDP ctxs to the new media PDP ctxs when the dropped session are re-established, after new S-CSCF has been selected. This behaviour

cannot be subject to standardisation and is completely implementation dependant. It is therefore not further outlined here, but should be generally claimed in the IPR.

It needs to be noted that there is another kind of S-CSCF re-selection, that takes place during initial registration (see 24.229). The I-CSCF in this case would try to contact the second S-CSCF after the first S-CSCF has timed out. Therefore the I-CSCF needs to be able to differentiate between an initial and a re-registration. This can be done by the "integrity-protected" flag in the REGISTER request, that is set by the P-CSCF. A request is only sent integrity protected when a Security Association between the UE and the P-CSCF has been established. This SA can only be established during successful authentication / registration. Therefore the absence of the "integrity-protected" flag indicates, that the REGISTER is an initial REGISTER request. I.e. the I-CSCF behaviour would be

- IF integrity protected flag present AND S-CSCF is not responding send 504.
- IF integrity protected flag NOT present AND S-CSCF is not responding ask capabilities and select S-CSCF

### **3. Advantages and disadvantages**

- + solves all problems for the case of S-CSCF out-of-order
- + clear all UE and network states
- + easy procedure, as completely built on existing (initial registration) procedures.

### **4. List of abbreviations**

CSCF – Call Session Control Function

IMS – IP Multimedia Core Network Subsystem

SIP – Session Initiation Protocol

UE – User Equipment

S-CSCF – Serving Call Session Control Function

P-CSCF – Proxy Call Session Control Function

I- CSCF – Interrogating Call Session Control Function

AS – Application Server

## **DESCRIPTION OF THE INVENTION**

### **5. Field of technology and background**

SIP is the Session Initiation Protocol as defined by the IETF in RFC 3261. It allows the establishment, handling and release of end-to-end multimedia sessions. There are several additions to the SIP protocol, which e.g. allow event notification based on SIP, which is the basis for a SIP based Presence Service and other services.

IMS is the 3GPP IP Multimedia Subsystem, that makes use of SIP as its call control protocol. See TS 23.228, 24.229 and 24.228.

### **6. Problem**

Scenario: A user has successfully registered to the S-CSCF and was authenticated. During the user's active registration, the S-CSCF goes out of service.

Problems:

- How can another S-CSCF be selected by the I-CSCF?
- How can I-CSCF separate between re-registration and initial registration?

## 7. Invention

From a UE perspective change of S-CSCF on the fly during re-registration would be technically possible. However it is not considered desirable because UE would need to realise the change from the re-registration response (i.e. 200 OK) e.g. the value service route has been changed. The planned behaviour of I-CSCF during a re-registration is: if the S-CSCF is not responding then the I-CSCF would reject the re-registration with an appropriate SIP error message.

When the UE then decides to start an initial registration to clear states in the UE and in the network then the I-CSCF needs to differentiate that this is not re-registration (which would cause sending a SIP error message). This is needed for avoiding endless loop.

Therefore, it would be desirable to instruct the UE to perform an initial registration when the UE is performing re-registration. An initial registration would clean-up states in the UE and in the network.

This can be done by the "integrity-protected" flag in the REGISTER request that is set by the P-CSCF. A request is only sent integrity protected when a Security Association (SA) between the UE and the P-CSCF has been established. This SA can only be established during successful authentication / registration. Therefore the absence of the "integrity-protected" flag indicates, that the REGISTER is an initial REGISTER request. I.e. the I-CSCF behaviour would be

- IF integrity protected flag present AND S-CSCF is not responding send 504.
- IF integrity protected flag NOT present AND S-CSCF is not responding ask capabilities and select S-CSCF

## 8. Advantages and disadvantages

- + allows possibility to change S-CSCF
- + increase redundancy in the network
- + makes possible to safely to shut down a network entity and guidance all UEs to a different network entity (i.e. prevent S-CSCF to respond REGISTER request and by removing S-CSCF from I-CSCF selection list)

List of abbreviations

CSCF – Call Session Control Function  
 IMS – IP Multimedia Core Network Subsystem  
 SIP – Session Initiation Protocol

### Problem description

24.229 currently only describes a case of S-CSCF re-selection that works when no other dialogs are ongoing via the S-CSCF that does not respond. In this case, the I-CSCF can easily re-select a new S-CSCF.

If the UE has already dialogs established, all these dialogs have to be dropped, in order to ensure correct network and UE behaviour. This is due to the fact, that the S-CSCF (which went out-of-order) has record-routed to every dialog that was established from/to its user. This means further, that no requests or responses on these dialogs will ever reach the user or can be sent from the user, when this S-CSCF is out of order.

24.229 also does not state what happens, if not the I-CSCF (chapter 5.3) but the P-CSCF (chapter 5.2) gets aware of a S-CSCF being out of order. It must be said that in most of the cases the P-CSCF will detect that the S-CSCF is out of order, as the I-CSCF only handles REGISTER requests.

Additionally also the procedures for P-CSCF re-selection need to be described for the case the P-CSCF goes out of order.

### Proposal

The following procedures are proposed:

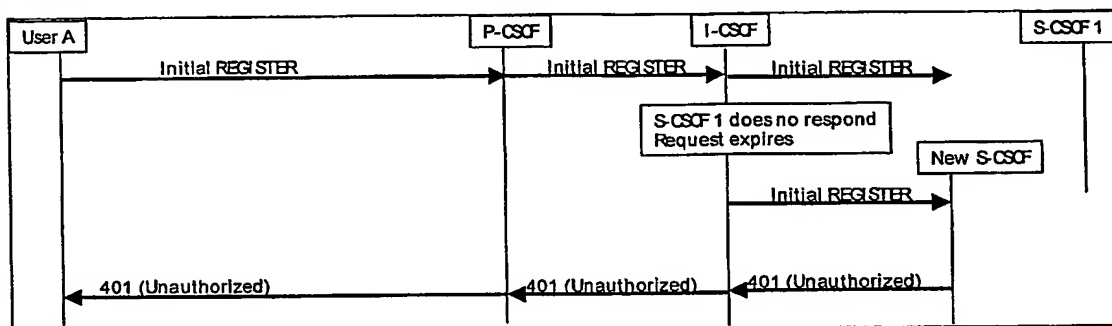
1. If the UE detects that its S-CSCF is out of order, it shall behave as if it has been re-booted, i.e. it drops the signalling and all related media PDP contexts and establishes a new signalling PDP context afterwards and performs initial registration again. Only with this procedure it can be guaranteed that all dialogs are cleared.

*Note: If the UE keeps the PDP contexts, it will not be able to perform any SIP based functionality – it will not be able to send or receive any SIP message. Furthermore the charging related data generated in the network will not be in-line with the real user behaviour.*

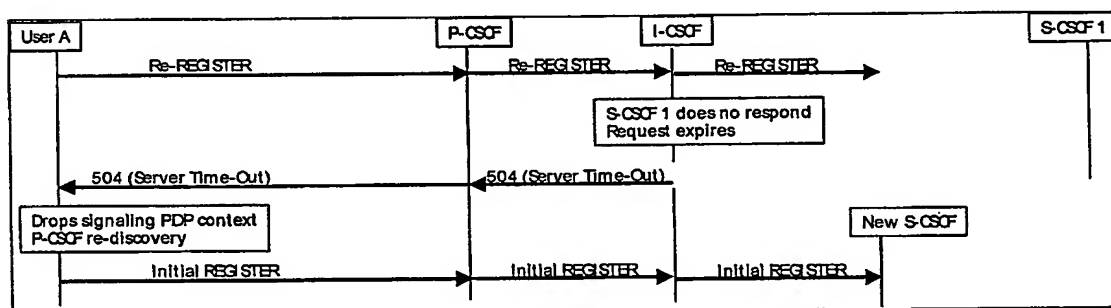
2. The I-CSCF needs to differentiate between initial REGISTER requests (for these registrations it can be sure, that no dialogs exist via the S-CSCF) and re-REGISTER requests:
  - a. this differentiation will be based on the "integrity-protected" flag in the Authorization header;
  - b. in case of an initial REGISTER that is not responded to, the I-CSCF behaviour does not change from the procedures as they are already described in 24.229, i.e. the I-CSCF just re-selects a new S-CSCF;
  - c. in case of a re-REGISTER that is not responded to, the I-CSCF shall return a 504 (Server Time-Out) response to the UE.
3. The UE detects that its S-CSCF is out of order when it receives a 504 (Server Time-Out) response for a REGISTER request and performs the actions stated in item 1.
4. If a request sent from the P-CSCF towards the network times out, the P-CSCF also returns a 504 (Server Time-Out) response. If this response is received by the UE, the UE cannot be sure if it was its own S-CSCF that went out of order or another server or the route. In order to get aware, whether its own S-CSCF went out of order, it shall perform re-registration procedures.

The UE shall behave in the same way as in (1), if it is unable to send a SIP request towards the P-CSCF.

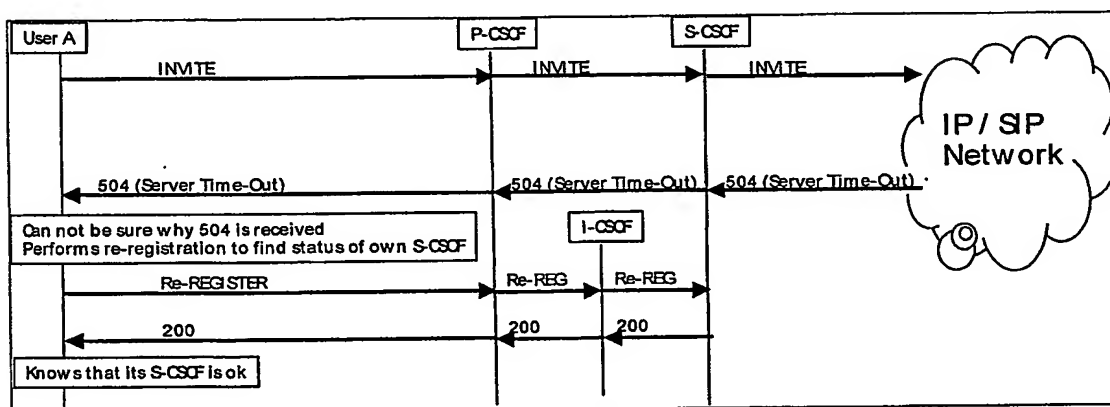
**Example Flow: S-CSCF re-selection during initial registration – I-CSCF selects new S-CSCF**



**Example Flow: S-CSCF re-selection during re-registration – UE drops IMS related PDP contexts**

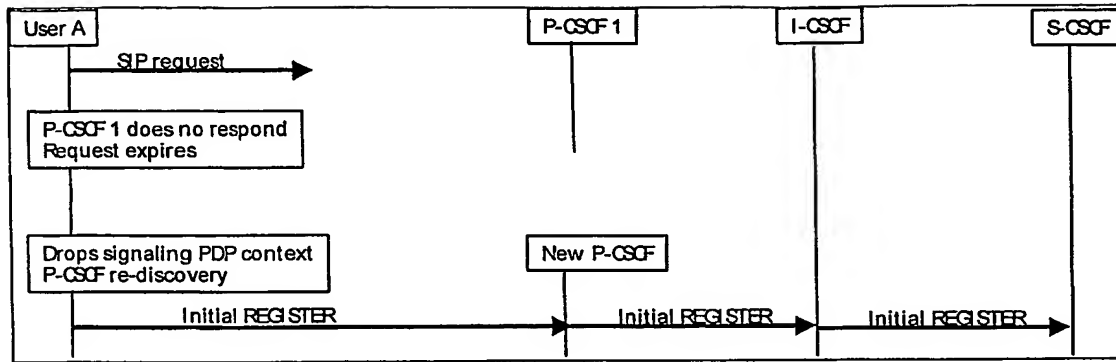


**Example Flow: P-CSCF sends 504 response**



**Example Flow: P-CSCF re-selection**





**Reason for change:** 24.229 currently only describes a case of S-CSCF re-selection that works when no other dialogs are ongoing via the S-CSCF that does not respond. In this case, the I-CSCF can easily re-select a new S-CSCF.

If the UE has already dialogs established, all these dialogs have to be dropped, in order to ensure correct network and UE behaviour. This is due to the fact, that the S-CSCF (which went out-of-order) has record-routed to every dialog that was established from/to its user. This means further, that no requests or responses on these dialogs will ever reach the user or can be sent from the user, when this S-CSCF is out of order.

24.229 also does not state what happens, if not the I-CSCF (chapter 5.3) but the P-CSCF (chapter 5.2) gets aware of a S-CSCF being out of order. It must be said that in most of the cases the P-CSCF will detect that the S-CSCF is out of order, as the I-CSCF only handles REGISTER requests.

Additionally also the procedures for P-CSCF re-selection need to be described.

**Summary of change:** 1. If the UE detects that its S-CSCF is out of order, it shall behave as if it has been re-booted, i.e. it drops the signalling and all related media PDP contexts and establishes a new signalling PDP context afterwards and performs initial registration again. Only with this procedure it can be guaranteed that all dialogs are cleared.

Note: If the UE would keep the PDP contexts, it will not be able to perform any SIP based functionality – it will not be able to send or receive any SIP message. Furthermore the charging related data generated in the network will not be in-line with the real user behaviour.

2. The I-CSCF needs to differentiate between initial REGISTER requests (for these registrations it can be sure, that no dialogs exist via the S-CSCF) and re-REGISTER requests:

a) this differentiation will be based on the "integrity-protected" flag in the Authorization header;

b) in case of an initial REGISTER that is not responded to, the I-CSCF behaviour does not change from the procedures as they are already

described in 24.229, i.e. the I-CSCF just re-selects a new S-CSCF;

c) in case of a re-REGISTER that is not responded to, the I-CSCF shall return a 504 (Server Time-Out) response to the UE.

3. The UE detects that its S-CSCF is out of order when it receives a 504 (Server Time-Out) response for a REGISTER request and performs the actions stated in bullet 1.

4. If a request sent from the P-CSCF towards the network times out, the P-CSCF also returns a 504 (Server Time-Out) response. If this response is received by the UE, the UE cannot be sure if it was its own S-CSCF that went out of order or another server or the route. In order to get aware, whether its own S-CSCF went out of order, it shall perform re-registration procedures.

The UE shall behave in the same way as in (1), if it is unable to send a SIP request towards the P-CSCF

***Consequences if not approved:***

⌘ S-CSCF reselection procedures are not complete and wrong (as they are stated now).

S-CSCF reselection will not work in case of S-CSCF going out of order whilst user is already registered. Dialogs / transactions states will stay inside the network.

Wrong charging information will be generated.

#### 5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less.

The UE shall protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if IK is available.

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

- a) an Authorization header, with the username field set to the value of the private user identity;
- b) a From header set to the SIP URI that contains the public user identity to be registered;
- c) a To header set to the SIP URI that contains the public user identity to be registered;
- d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

- e) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

- f) a Request-URI set to the SIP URI of the domain name of the home network;
- g) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];
- h) the Supported header containing the option tag "path"; and
- i) the P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- a) store the new expiration time of the registration for this public user identity found in the To header value;
- b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

- c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and
- d) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

When receiving a 504 (Server Time-Out) response to the REGISTER request the UE shall

- 1) stop local processing of all ongoing SIP related dialogs and transactions and drop them locally;
- 2) drop the signalling IP-CAN bearer;
- 3) drop all related IP-CAN bearers that were established for transport of media;
- 4) establish a new signalling IP-CAN bearer; and
- 5) perform the actions for initial registration as described in subclause 5.1.1.2.

When the REGISTER request cannot be sent towards the P-CSCF (e.g. times out), the UE shall stop local processing of all ongoing SIP related dialogs and transactions and drop them locally; and either try to connect to the other P-CSCFs whose addresses were received during the P-CSCF discovery procedure; or

- 1) drop the signalling IP-CAN bearer;
- 2) drop all related IP-CAN bearers that were established for transport of media;
- 3) establish a new signalling IP-CAN bearer; and
- 4) perform the actions for initial registration as described in subclause 5.1.1.2.

## ~~Second Change~~

### 5.1.2A Generic procedures applicable to all methods excluding the REGISTER method

#### 5.1.2A.1 Mobile-originating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

The UE shall discard any SIP message that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

In accordance with RFC 3325 [34] the UE may insert a P-Preferred-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the P-Preferred-Identity header:

- a public user identity which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implicit registration that was not subsequently deregistered or has expired; or

- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 1: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header.

NOTE 2: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header to "Anonymous".

NOTE 3: The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is explicitly required. As the user may well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header from the public user identity or other values stored in or derived from the UICC. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header other than Anonymous.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34]. The UE shall insert a P-Access-Network-Info header into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

On receiving a 504 (Server Time-Out) response to a request, the UE shall perform the procedures for re-registration as described in subclause 5.1.1.4.

**If a request cannot be sent towards the P-CSCF, the UE shall behave as if a request could not be sent towards the P-CSCF, as described in subclause 5.1.1.4.5.1.2A.2 Mobile-terminating case**

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

The UE shall discard any SIP message that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

NOTE 1: In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Preferred-Identity in the form of a hint.

The UE shall insert a P-Access-Network-Info header into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a

dialog or any response to a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

### ~Third Change~

#### 5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

1) insert a Path header in the request including an entry containing:

- the SIP URI identifying the P-CSCF;
- an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

2) insert a Require header containing the option tag "path";

3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header;

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication response, or it was received on the security association created during the last successful authentication procedure and with no authentication response, otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

- check the security association which protected the request. If that has a temporary lifetime, and the REGISTER request was received protected with the new security association, then the request shall contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
- if the security association the REGISTER request was received on, is an already established one, then:
  - a Security-Verify header is not expected to be included. If the Security-Verify header is present, then the P-CSCF shall remove that header together with the 'Require: sec-agree' header;

- a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
  - the P-CSCF shall remove the Security-Client header before forwarding the request to the S-CSCF; and
  - check if the private user identity conveyed in the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;
- 7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and
- 8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;
- 2) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms. The P-CSCF shall support the setup of two pairs of security associations. For further information see 3GPP TS 33.203 [19]; and
- 3) set up the new security associations with a temporary lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set a temporary SIP level lifetime for the security association which has to be long enough to permit the UE to finalize the registration procedure (bigger than 64\*T1).
- 4) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- 1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routing information in the requests originated by the UE. If this

registration is a re-registration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

- 2) associate the Service-Route header list with the registered public user identity;
- 3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;
- 4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more than one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

- 5) store the values received in the P-Charging-Function-Addresses header;
- 6) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- 7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

The P-CSCF shall:

- if new security associations are established and there are no old security associations, start using the new security associations towards the UE after the 200 (OK) has been sent out;
- if a request protected within the newly established security associations is received from a UE which has old security associations, delete the old security associations and related keys when all SIP transactions that use the old security associations are completed;
- if the newly established security associations has not been taken into use by the UE and the UE sends request protected on the old security associations, delete the new security associations; and
- if the newly established security associations are a result of an unprotected REGISTER request being received from the UE, then delete the old security associations which may exist towards the UE.

NOTE 3: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

If no response is received for the sent REGISTER request and its retransmissions by the P-CSCF, the P-CSCF may send back a 503 (Service Unavailable) response to the user. The 503 (Service Unavailable) response may contain a Retry-After header specifying a time interval after which the UE can resend the request.



~~Fourth Change~~

**5.2.6 General treatment for all dialogs and standalone transactions excluding the REGISTER method**

**5.2.6.1 Introduction**

The procedures of subclause 5.2.6 and its subclauses are general to all requests and responses, except those for the REGISTER method.

**5.2.6.2 Determination of mobile-originated or mobile-terminated case**

Upon receipt of an initial request or a target refresh request or a stand-alone transaction, the P-CSCF shall:

- perform the procedures for the mobile-terminating case as described in subclause 5.2.6.4 if the request makes use of the information for mobile-terminating calls, which was added to the Path header entry of the P-CSCF during registration (see subclause 5.2.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter;
- perform the procedures for the mobile-originating case as described in subclause 5.2.6.3 if this information is not used by the request.

**5.2.6.3 Requests initiated by the UE**

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more than one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 1: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
  - b) replace the preloaded Route header value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or re-registration;
- 2) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:
  - a) the P-CSCF FQDN that resolves to the IP address, or
  - b) the P-CSCF IP address;

- 3) add its own SIP URI to the top of the Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:
  - a) the P-CSCF FQDN that resolves to the IP address; or
  - b) the P-CSCF IP address;
- 4) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;
- 5) create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
- 6) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header;
- 2) store the list of Record-Route headers from the received response;
- 3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;
- 4) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port values see 3GPP TS 33.203 [19].

- 5) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE a target refresh request for a dialog, the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
  - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;
  - b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;
- 2) verify that the list of Route headers in the request is included, in the list of Record-Route headers that was received during the last target refresh request for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

- a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
  - b) replace the Route header value in the request with the one received during the last target refresh request for the same dialog in the Record-Route header;
- 3) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:
- a) the P-CSCF FQDN that resolves to the IP address, or
  - b) the P-CSCF IP address;
- 4) add its own SIP URI to the top of Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:
- a) the P-CSCF FQDN that resolves to the IP address; or
  - b) the P-CSCF IP address; and
- 5) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the list of Record-Route headers from the received response;
- 2) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

**NOTE 3:** The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

- 3) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for a standalone transaction, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
  - b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;

- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and
- 3) create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
  - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;
  - b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps; and
- 2) verify that the list of Route headers in the request matches the list of Record-Route headers that was received during the last target refresh request for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
  - b) replace the Route header value in the request with the one received during the last target refresh request for the same dialog in the Record-Route header;

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for an unknown method (that does not relate to an existing dialog), and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
  - b) replace the Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response; and
- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

If no response is received for a sent request and its retransmissions by the P-CSCF, the P-CSCF may send back a 504 (Server Time-Out) response to the user, forcing the UE to behave as described in subclause 5.1.1.4.

### ~~Fifth change~~

#### 5.3.1 Registration procedure

##### 5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

##### 5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

- 1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;
- 2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

- 1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more than one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;
- 2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;
- 3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.

##### 5.3.1.3 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 403 (Forbidden) response to the UE. The response may include a Warning header containing the warn-code 399.

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 (Forbidden) response. The response may include a Warning header containing the warn-code 399.

If the user registration status query procedure cannot be completed, e.g. due to time-out or incorrect information from the HSS, the I-CSCF shall send back a 480 (Temporarily Unavailable) response to the UE.

If a selected S-CSCF:

- does not respond to the REGISTER request and its retransmissions by the I-CSCF and the REGISTER request did not include an "integrity-protected" parameter in the Authorization header or did include an "integrity-protected" parameter with a value different from "yes"; or
- sends back a 3xx response or 480 (Temporarily Unavailable) response;

the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

If a selected S-CSCF does not respond to a REGISTER request and its retransmissions by the I-CSCF and the REGISTER request did include an Authorization header with the "integrity-protected" parameter set to "yes", the I-CSCF shall send back a 504 (Server Time-Out) response to the user.

If the I-CSCF cannot select a S-CSCF which fulfils the mandatory capabilities indicated by the HSS, the I-CSCF shall send back a 600 (Busy Everywhere) response to the user.

***Reason for change:***

24.229 currently only describes a case of S-CSCF re-selection that works when no other dialogs are ongoing via the S-CSCF that does not respond. In this case, the I-CSCF can easily re-select a new S-CSCF.

If the UE has already dialogs established, all these dialogs have to be dropped, in order to ensure correct network and UE behaviour. This is due to the fact, that the S-CSCF (which went out-of-order) has record-routed to every dialog that was established from/to its user. This means further, that no requests or responses on these dialogs will ever reach the user or can be sent from the user, when this S-CSCF is out of order.

24.229 also does not state what happens, if not the I-CSCF (chapter 5.3) but the P-CSCF (chapter 5.2) gets aware of a S-CSCF being out of order. It must be said that in most of the cases the P-CSCF will detect that the S-CSCF is out of order, as the I-CSCF only handles REGISTER requests.

Additionally also the procedures for P-CSCF re-selection need to be described.

***Summary of change:***

1. If the UE detects that its S-CSCF is out of order, it shall behave as if it has been re-booted, i.e. it drops the signalling and all related media PDP contexts and establishes a new signalling PDP context afterwards and performs initial registration again. Only with this procedure it can be guaranteed that all dialogs are cleared

Note: If the UE would keep the PDP contexts, it will not be able to perform any SIP based functionality – it will not be able to send or receive any SIP message. Furthermore the charging related data generated in the network will not be in-line with the real user behaviour.

2. The I-CSCF needs to differentiate between initial REGISTER requests (for these registrations it can be sure, that no dialogs exist via the S-CSCF) and re-REGISTER requests:

a) this differentiation will be based on the "integrity-protected" flag

in the Authorization header

b) in case of an initial REGISTER that is not responded to, the I-CSCF behaviour does not change from the procedures as they are already described in 24.229, i.e. the I-CSCF just re-selects a new S-CSCF.

c) in case of a re-REGISTER that is not responded to, the I-CSCF shall return a 504 (Server Time-Out) response to the UE.

3. The UE detects that its S-CSCF is out of order when it receives a 504 (Server Time-Out) response for a REGISTER request and performs the actions stated in bullet 1.

4. If a request sent from the P-CSCF towards the network times out, the P-CSCF also returns a 504 (Server Time-Out) response. If this response is received by the UE, the UE cannot be sure if it was its own S-CSCF that went out of order or another server or the route. In order to get aware, whether its own S-CSCF went out of order, it shall perform re-registration procedures.

The UE shall behave in the same way as in (1), if it is unable to send a SIP request towards the P-CSCF

***Consequences if not approved:***

S-CSCF reselection procedures are not complete and wrong (as they are stated now).

S-CSCF reselection will not work in case of S-CSCF going out of order whilst user is already registered. Dialogs / transactions states will stay inside the network.

Wrong charging information will be generated.

**~~First Change~~**

**5.1.1.4 User-initiated re-registration**

The UE can reregister a previously registered public user identity at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less.

The UE shall protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if IK is available.

The UE shall extract or derive from the  $UICC$  a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

- a) an Authorization header, with the username field set to the value of the private user identity;
- b) a From header set to the SIP URI that contains the public user identity to be registered;
- c) a To header set to the SIP URI that contains the public user identity to be registered;

- d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

- e) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

- f) a Request-URI set to the SIP URI of the domain name of the home network;
- g) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];
- h) the Supported header containing the option tag "path"; and
- i) the P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- a) store the new expiration time of the registration for this public user identity found in the To header value;
- b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;
- c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and
- d) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

When receiving a 504 (Server Time-Out) response to the REGISTER request the UE shall

- 1) stop local processing of all ongoing SIP related dialogs and transactions and drop them locally;
- 2) drop the signalling IP-CAN bearer;
- 3) drop all related IP-CAN bearers that were established for transport of media;



4) establish a new signalling IP-CAN bearer; and

5) perform the actions for initial registration as described in subclause 5.1.1.2.

When the REGISTER request cannot be sent towards the P-CSCF (e.g. times out), the UE shall stop local processing of all ongoing SIP related dialogs and transactions and drop them locally; and either try to connect to the other P-CSCFs whose addresses were received during the P-CSCF discovery procedure; or

1) drop the signalling IP-CAN bearer;

2) drop all related IP-CAN bearers that were established for transport of media;

3) establish a new signalling IP-CAN bearer; and

4) perform the actions for initial registration as described in subclause 5.1.1.2.

#### ~~Second Change~~

5.1.2A Generic procedures applicable to all methods excluding the REGISTER method

##### 5.1.2A.1 Mobile-originating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

The UE shall discard any SIP message that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

In accordance with RFC 3325 [34] the UE may insert a P-Preferred-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the P-Preferred-Identity header:

- a public user identity which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implicit registration that was not subsequently deregistered or has expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 1: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header.

NOTE 2: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header to "Anonymous".

**NOTE 3:** The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is explicitly required. As the user may well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header from the public user identity or other values stored in or derived from the UICC. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header other than Anonymous.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34]. The UE shall insert a P-Access-Network-Info header into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4). The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration. On receiving a 504 (Server Time-Out) response to a request, the UE shall perform the procedures for re-registration as described in subclause 5.1.1.4.

If a request cannot be sent towards the P-CSCF, the UE shall behave as if a request could not be sent towards the P-CSCF, as described in subclause 5.1.1.4.

#### **5.1.2A.2 Mobile-terminating case**

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

The UE shall discard any SIP message that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

**NOTE 1:** In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Preferred-Identity in the form of a hint.

The UE shall insert a P-Access-Network-Info header into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

~~Third Change~~

#### **5.2.2 Registration**

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

1) insert a Path header in the request including an entry containing:

- the SIP URI identifying the P-CSCF;
- an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may

e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

- 2) insert a Require header containing the option tag "path";
- 3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header;
- 4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication response, or it was received on the security association created during the last successful authentication procedure and with no authentication response, otherwise insert the parameter with the value "no";
- 5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;
- 6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:
  - check the security association which protected the request. If that has a temporary lifetime, and the REGISTER request was received protected with the new security association, then the request shall contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
  - if the security association the REGISTER request was received on, is an already established one, then:
    - a Security-Verify header is not expected to be included. If the Security-Verify header is present, then the P-CSCF shall remove that header together with the 'Require: sec-agree' header;
    - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
    - the P-CSCF shall remove the Security-Client header before forwarding the request to the S-CSCF; and
  - check if the private user identity conveyed in the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

- 7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and
- 8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;
- 2) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms. The P-CSCF shall support the setup of two pairs of security associations. For further information see 3GPP TS 33.203 [19]; and
- 3) set up the new security associations with a temporary lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set a temporary SIP level lifetime for the security association which has to be long enough to permit the UE to finalize the registration procedure (bigger than  $64 \cdot T1$ ).
- 4) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- 1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;
- 2) associate the Service-Route header list with the registered public user identity;
- 3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;
- 4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more than one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

- 5) store the values received in the P-Charging-Function-Addresses header;
- 6) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- 7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

The P-CSCF shall:

- if new security associations are established and there are no old security associations, start using the new security associations towards the UE after the 200 (OK) has been sent out;
- if a request protected within the newly established security associations is received from a UE which has old security associations, delete the old security associations and related keys when all SIP transactions that use the old security associations are completed;
- if the newly established security associations has not been taken into use by the UE and the UE sends request protected on the old security associations, delete the new security associations; and
- if the newly established security associations are a result of an unprotected REGISTER request being received from the UE, then delete the old security associations which may exist towards the UE.

NOTE 3: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

If no response is received for the sent REGISTER request and its retransmissions by the P-CSCF, the P-CSCF may send back a 503 (Service Unavailable) response to the user. The 503 (Service Unavailable) response may contain a Retry-After header specifying a time interval after which the UE can resend the request.

~~ Fourth Change ~~

5.2.6 General treatment for all dialogs and standalone transactions excluding the REGISTER method

#### 5.2.6.1 Introduction

The procedures of subclause 5.2.6 and its subclauses are general to all requests and responses, except those for the REGISTER method.

#### 5.2.6.2 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a target refresh request or a stand-alone transaction, the P-CSCF shall:

- perform the procedures for the mobile-terminating case as described in subclause 5.2.6.4 if the request makes use of the information for mobile-terminating calls, which was added to the Path header entry of the P-CSCF during registration (see subclause 5.2.2), e.g. the message is

received at a certain port or the topmost Route header contains a specific user part or parameter;

- perform the procedures for the mobile-originating case as described in subclause 5.2.6.3 if this information is not used by the request.

### 5.2.6.3 Requests initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains as P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more than one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 1: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
  - b) replace the preloaded Route header value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or reregistration;
- 2) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:
  - a) the P-CSCF FQDN that resolves to the IP address, or
  - b) the P-CSCF IP address;
- 3) add its own SIP URI to the top of the Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:
  - a) the P-CSCF FQDN that resolves to the IP address; or
  - b) the P-CSCF IP address;
- 4) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;
- 5) create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
- 6) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header;
- 2) store the list of Record-Route headers from the received response;
- 3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;
- 4) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port values see 3GPP TS 33.203 [19].

- 5) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE a target refresh request for a dialog, the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
  - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;
  - b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;
- 2) verify that the list of Route headers in the request is included, in the list of Record-Route headers that was received during the last target refresh request for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
  - b) replace the Route header value in the request with the one received during the last target refresh request for the same dialog in the Record-Route header;
- 3) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:
  - a) the P-CSCF FQDN that resolves to the IP address, or
  - b) the P-CSCF IP address;
- 4) add its own SIP URI to the top of Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

- a) the P-CSCF FQDN that resolves to the IP address; or
- b) the P-CSCF IP address; and

- 5) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the list of Record-Route headers from the received response;
- 2) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

- 3) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for a standalone transaction, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
  - b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;
- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and
- 3) create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
  - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the



originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;

- b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps; and
- 2) verify that the list of Route headers in the request matches the list of Record-Route headers that was received during the last target refresh request for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
  - b) replace the Route header value in the request with the one received during the last target refresh request for the same dialog in the Record-Route header;

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for an unknown method (that does not relate to an existing dialog), and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
  - b) replace the Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response; and
- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

If no response is received for a sent request and its retransmissions by the P-CSCF, the P-CSCF may send back a 504 (Server Time-Out) response to the user, forcing the UE to behave as described in subclause 5.1.1.4.

~~Fifth and last Change~~

### 5.3.1 Registration procedure

#### 5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

#### 5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

NOTE: One IMS user may register the same IMS public user identity from different terminals. These registrations from the same user are directed to the same S-CSCF as described in 3GPP TS 29.228 [14].

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

- 1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;
- 2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

- 1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more than one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;
- 2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;
- 3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.

#### **5.3.1.3 Abnormal cases**

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 403 (Forbidden) response to the UE. The response may include a Warning header containing the warn-code 399.

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 (Forbidden) response. The response may include a Warning header containing the warn-code 399.

If the user registration status query procedure cannot be completed, e.g. due to time-out or incorrect information from the HSS, the I-CSCF shall send back a 480 (Temporarily Unavailable) response to the UE.

If a selected S-CSCF:

- does not respond to the REGISTER request and its retransmissions by the I-CSCF and the REGISTER request did not include an "integrity-protected" parameter in the Authorization header or did include an "integrity-protected" parameter with a value different from "yes"; or
- sends back a 3xx response or 480 (Temporarily Unavailable) response;

the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

If a selected S-CSCF does not respond to a REGISTER request and its retransmissions by the I-CSCF and the REGISTER request did include an Authorization header with the "integrity-protected" parameter set to "yes", the I-CSCF shall send back a 504 (Server Time-Out) response to the user.

If the I-CSCF cannot select a S-CSCF which fulfils the mandatory capabilities indicated by the HSS, the I-CSCF shall send back a 600 (Busy Everywhere) response to the user.

The applicant hereby discloses that the invention is not to be interpreted solely on the scope of claims.

It is understood that the term out of service can be interpreted as meaning that either the serving network element is not communicating with said user equipment due to a fault in the serving network element, or a fault in the communications network preventing the user equipment communicating the serving network element.

Furthermore it is understood that the user equipment can comprises mobile phones, personal communication devices, and personal data assistants.

It is further understood that the act of establishing a bearer for signalling can be understood to mean creating a communication session, and wherein the communication node is arranged to be capable of communication with a network by means of a communication session, the network comprising a session authorisation node for authorising establishment of a communication session; the communication node being arranged to, in order to establish a session, communicate with the session authorisation node for receiving authorisation of the session; the communication node being capable of, during a communication session, requesting the authorisation node for authorisation of the session and being arranged to terminate at least the signalling of the session in response to receiving from the network in response to such a request a message indicating a failure by the session authorisation node to respond to the request.

The applicant hereby discloses in isolation each individual feature described herein and any combination of two or more such features, to the extent that such features or combinations are capable of being carried out based on the present specification as a whole in the light of the common general knowledge of a person skilled in the art, irrespective of whether such features or combinations of features solve any problems disclosed herein, and without limitation to the scope of the claims. The applicant indicates that aspects of the present invention may consist of any such individual feature or combination of features. In view of the foregoing description it will be evident to a person skilled in the art that various modifications may be made within the scope of the invention.

Claims:

1. A method for handling service failures in a communications network, the method comprising the steps of:
  - (a) establishing a bearer for signalling between a user equipment and the communications network,
  - (b) registering as a first type of registration the user equipment to a serving network element in a communications network,
  - (c) detecting by a first network element that the serving network element in a communications network is out of service,
  - (d) sending from the first network element to the user equipment a message including an indication that the serving network element is out of service.
2. A method of claim 1 or 3, further comprising the step of:
  - (a) initiating a registration of a second type by the user equipment to the communications network.
3. A method according to claim 1 comprising the further step of:
  - (a) receiving by the user equipment an indication from the first network element that a network element is out of service in a communications network in response to a message sent by the user equipment.
4. A method of any of the claims 1 to 3 wherein the first network element is a P-CSCF.
5. A method according to claim 2, further comprising the steps of:
  - (b) detecting by a first network element that the serving network element is out of service during the second type of registration,
  - (d) dropping the bearer for signalling by the user equipment in response to receiving the message from the first network element,
  - (e) registering a first type of registration to the communications network by the user equipment,
  - (f) establishing a second bearer for signalling between the user equipment and the communications network.

6. A method according to claim 1, 2 or 5, wherein the bearer for signalling is a signalling or general purpose PDP context, the communications network is an IMS network, the first type of registration is an initial registration, the second type of registration is a re-registration, the first network element is an Interrogating CSCF (I-CSCF) and the serving network element is a S-CSCF.

7. A method for determining a type of registration in a communications network comprising the steps of:

- (a). sending a request for register from an user equipment to a first network element,
- (b). checking in the first network element an information element in the request,
- (c). determining based on said result of the checking step, if the register request is for a first type of registration or for a second type of registration.

8. A method according to claim 7, comprising further steps of:

- (a). receiving no response from a serving network element,
- (b). sending an serving network element out of service message to the UE, if the register request is for first type of registration,
- (c). selecting a new serving network element by the first network element if the register request is for the second type of registration.

9. A method according to claim 7, wherein the first type of registration is a re-registration and the second type of registration is an initial registration.

10. A method according to claim 7, wherein the checking step is checking the presence of the information element in the request.

11. A method according to any of claims 7 to 10, wherein the information element indicates that the request is sent integrity protected.

12. A method according to any of claims 7 to 11, wherein the information indicates that the user has been successfully authenticated.

13. A method of claim 7, wherein the information in the request is an integrity protected flag.

14. A network element in a communications network arranged to have means for sending message to and/or from a serving network element, means for detecting the information that serving

network element is not capable of serving an user equipment and means for sending the information to the user equipment.

15. A network element in a communications network arranged to have means for receiving registration request and means for checking if the registration request is of a first type or a second type.

16. A network element in a communications network arranged to have means for receiving messages from an user equipment and means for sending a message to the user equipment, the message indicating that a network element in the communications network is not capable of serving the user equipment.

17. A user equipment in a communications network arranged to have means for receiving a message from the communications network, the message indicating that the serving network element for the user equipment is not capable of serving the user equipment, and means for responding to the message by releasing bearers.

18. A user equipment of claim 17, wherein the user equipment is arranged to have means to perform initial registration for responding to the message.

**PCT/IB2004/003573**



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☒ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☒ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**